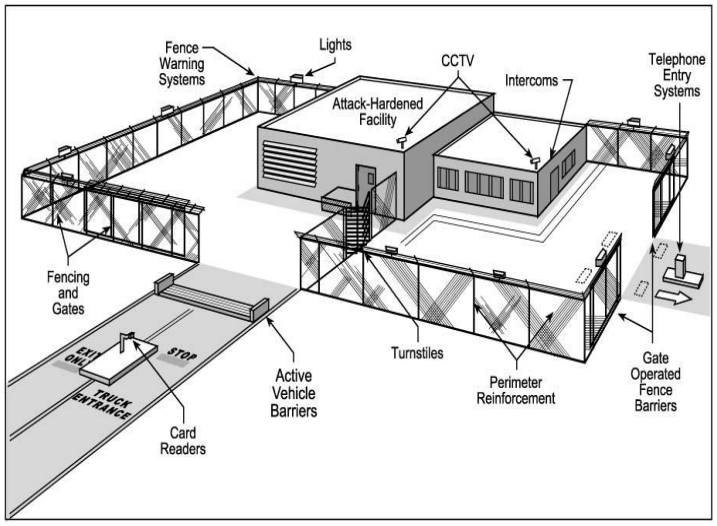
On-site Vulnerability and Physical Security Assessments

BACKGROUND

The Protective Design Center (PDC) has been executing various types of on-site antiterrorism/force protection and physical security assessments for nearly three decades. Vulnerability assessment customers include Defense Logistics Agency (DLA), Defense Contract Management Agency (DCMA), U.S. Military Recruiting Centers, U.S. Army Forces Command (FORSCOM), Defense Finance and Accounting Service (DFAS), Intelligence and Security Command (INSCOM), Army Corps of Engineers (USACE) and numerous military installations, among others. Vulnerability assessments vary in scope and are tailored to the specific needs of the customer. The on-site assessment process can be adapted to focus on hard assets (e.g., equipment, infrastructure), soft assets (e.g., personnel) or process/mission or a combination. Assessments also gauge compliance with applicable standards and regulations.



ASSESSMENT CAPABILITIES and OPTIONS

Current capabilities and options include:

- Antiterrorism/force protection (AT/FP)
- Physical Security
- Regulation and Standard Compliance
- Single or multiple building assessments
- Installation assessments
- DoD contractor facility assessments
- Locks/Dams & Power/Electrical Facility
- Critical Infrastructure assessments
- Access Control Point (ACP) assessments
- JSIVA style assessments
- Preliminary blast analysis, including simple building modeling using VAPO software
- In-depth blast analysis, including detailed building modeling and specialized computer analysis
- Intrusion Detection Systems (IDS) and CCTV, in conjunction with the Electronic Security Center
- Post-event Damage Assessments

AGGRESSOR THREAT TACTICS

Assessments can be tailored to consider a specific set of threat tactics, among which are:

- Moving and Stationary Vehicle Bomb Tactic
- Hand Delivered Explosives Tactic
- Direct Fire Weapons Attack Tactic
- Indirect Fire Weapons Tactic
- Forced Entry Tactic
- Covert Entry Tactic (e.g., false credentials)
- Insider Compromise Tactic (e.g., employee)
- Visual Surveillance
- Acoustic and Electronic Emanations Eavesdropping
- Airborne and Waterborne Contamination

PRESENTATION and REPORT OPTIONS

Intermediate and final products can be tailored to customer needs/requirements:

- In-brief prior to on-site assessment
- Out-brief to present preliminary findings immediately following on-site assessment (verbal, written, or PowerPoint presentation)
- Letter Report focusing on vulnerabilities and mitigating measures
- Draft Report to allow for customer review and comment prior to taking report to final
- Detailed Report documenting existing conditions; asset identification; aggressor tactics, weapons, and tools; vulnerabilities; mitigation recommendations and cost estimate; plans; photographs; threat analysis, incl. design basis threat (DBT) and recommended level of protection (LOP); preliminary blast analysis; and mitigating measure information cutsheets
- Antiterrorism (AT) Plans
- For Official Use Only (FOUO), classified, or FOUO with a classified annex

POINTS OF CONTACT

U.S. Army Corps of Engineers
Protective Design Center

Telephone:

Mr. Daniel Sommer, Chief, PDC	402-995-2376
Mr. Curt Betts, Chief, Security Engineering	402-995-2359
Mr. Thomas Schuberth, Project Manager	402-995-2374

Internet:
Web Page: https://pdc.usace.army.mil
email: thomas.f.schuberth@usace.army.mil

U.S. Army Corps of Engineers Protective Design Center